

Claims

The following is claimed:

1-26. (canceled)

27. (new) A computer-implemented method for creating a signature for subsequent authentication comprising the following steps:

indicating to a user commencement of signature input recording;

creating a signature by at least in part recording input signals by type from at least one user-selected device among a plurality of selectable user input devices,

wherein a signal comprises a set of related software-recognizable data of the same type received from at least one input device, and

wherein at least one user-selectable input device affords recording a plurality of signal types, and

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device.

28. (new) The method according to claim 27, wherein said recording comprises signals from a plurality of user-selected devices.

29. (new) The method according to claim 27, with the additional step of receiving user selection of at least one signal type from a plurality of signal types associated with at least one user input device.

30. (new) The method according to claim 27, with the additional step of passively terminating authentication comparison of a subsequent signature submission to said recording, thereby authenticating said subsequent signature.

31. (new) The method according to claim 27, with the following additional steps:
comparing a subsequent signature submission to said recording;
authenticating access even if said comparison results in an inexact match.
32. (new) The method according to claim 31, wherein the inexactness of said inexact match comprises a user-designated tolerance.
33. (new) The method according to claim 27, with the additional step of presenting at least a portion of said recording to said user for editing.
34. (new) The method according to claim 27, with the additional step of editing said recording.
35. (new) A computer-implemented method for creating a signature for subsequent authentication comprising:
receiving user selection of at least one signal type among a plurality of selectable signal types;
recording input data of at least one signal type from at least one user-selected input device among a plurality of selectable user input devices,
wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device,
and wherein at least one user-selectable input device affords recording a plurality of signal types;
creating a signature comprising at least in part said input data of said user-selected signal types.
36. (new) The method according to claim 35, wherein said recording comprises a plurality of user-selected devices.
37. (new) The method according to claim 35, such that said recording precedes said receiving signal type selection.

38. (new) The method according to claim 35, wherein at least one said signal type comprises input from a plurality of devices.

39. (new) The method according to claim 35, with the following additional steps:
comparing a subsequent signature submission to said recording;
authenticating access even if said comparison results in an inexact match.

40. (new) The method according to claim 35, with the additional step of editing said recording.

41. (new) The method according to claim 35, wherein said recording comprises a plurality of user-selected signal types.

42. (new) A computer-implemented method for incrementally authenticating a signature while receiving user input comprising:

iteratively receiving a plurality of portions of user input data and performing a corresponding authentication step for each portion,

wherein the first authentication step upon receiving a first portion of said user input comprises accumulating keys based upon matching correspondingly key data to said first portion of user input data,

wherein a key comprises at least in part a portion of a previously stored signature, said signature divisible into portions, said keys associating portions sequentially either integrally or by reference,

wherein, upon receiving each subsequent portion after said first portion, discarding from further processing previously accumulated keys based upon failure in matching respective key data to said user input data portion;

whereby continuing said iterative process until completing authentication by matching said last key to corresponding said user input data portion, or by process of elimination determining authentication impossible.

43. (new) The method according to claim 42, wherein accepting said match within a designated tolerance of inexactness.

44. (new) The method according to claim 42, wherein accessing at least one key by reference from another key.

45. (new) The method according to claim 42, wherein said first portion comprises input from a plurality of devices.

46. (new) A computer-implemented method for storing the signatures of a plurality of users comprising the following steps:

recording a plurality of signatures comprising data of a plurality of transmission types and signal types,

wherein a transmission type comprises indicia of a user-selected input device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device;

partitioning said signature data by transmission type and by signal type.

47. (new) The method according to claim 46, with the additional step of storing a signature at least in part by partitioning said signature into portions by signal type,

such that at least one portion references another portion of said signature.

48. (new) A computer-implemented method for creating a signature comprising the following steps:

recording user input of a plurality of signal types from at least one user-selected device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device;

receiving user selection among those signal types recorded,

whereby receiving user selection of at least one less signal type than recorded for said device;

creating a signature comprising at least in part said user-selected signal types.

49. (new) The method according to claim 48, with the additional step of receiving user indication to edit said signature.